ABSTRACT OF THE DISCLOSURE

An update utility requests a signature verification of the utility's signature along with a request to unlock the flash memory stored in the utility. A trusted platform module ("TPM") performs a signature verification of the utility using a previously stored public key. Upon verification of the signature, the TPM unlocks the flash memory to permit update of the utility. Upon completion of the update, the flash utility issues a lock request to the TPM to relock the flash memory.